

3-24-05

AF: [signature]  
\$

Express Mail Mailing Label No. ED535383777US

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Steven M. Blumenau, et al.

Serial No.: 10/058,651

Confirm: 5520

Filed: 01/28/2002

For: ELECTRONIC DEVICE FOR SECURE  
AUTHENTICATION OF OBJECTS  
SUCH AS COMPUTERS IN A DATA  
NETWORK

Group Art Unit: 2143

Examiner: Shin, Kyung H.

Atty. Dkt. No.: 10830.0033.DVUS01

**APPEAL BRIEF TO THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Commissioner for Patents  
PO Box 1450  
Alexandria, Virginia 22313-1450

Sir:

Please deduct the \$500. fee of 37 C.F.R. 41.20(b)(2) for filing a brief in support of the appeal from EMC Corporation Deposit Account No. 05-0889. A Fee transmittal form is enclosed for this purpose.

03/25/2005 BABRAHA1 00000084 050889 10058651  
02 FC:1402 500.00 DA

**I. REAL PARTY IN INTEREST**

The real party in interest is EMC Corporation, by virtue of an assignment recorded at Reel 9286 Frame 0570.

**II. RELATED APPEALS AND INTERFERENCES**

The appellants filed a Notice of Appeal (dated Feb. 26, 2002) and an Appeal Brief (dated April 26, 2002) in the parent application Ser. 09/107,202, resulting in the issuance of a Notice of

Allowance (dated July 29, 2002). The parent application issued on Dec. 10, 2002, as U.S. Patent 6,493,825. The parent application dealt with a method of authentication of a host processor requesting service in a data processing network. This method may use the electronic device that is the subject of the present application. There are no other related appeals or interferences.

### **III. STATUS OF CLAIMS**

Claims 1 to 12 have been presented for examination.

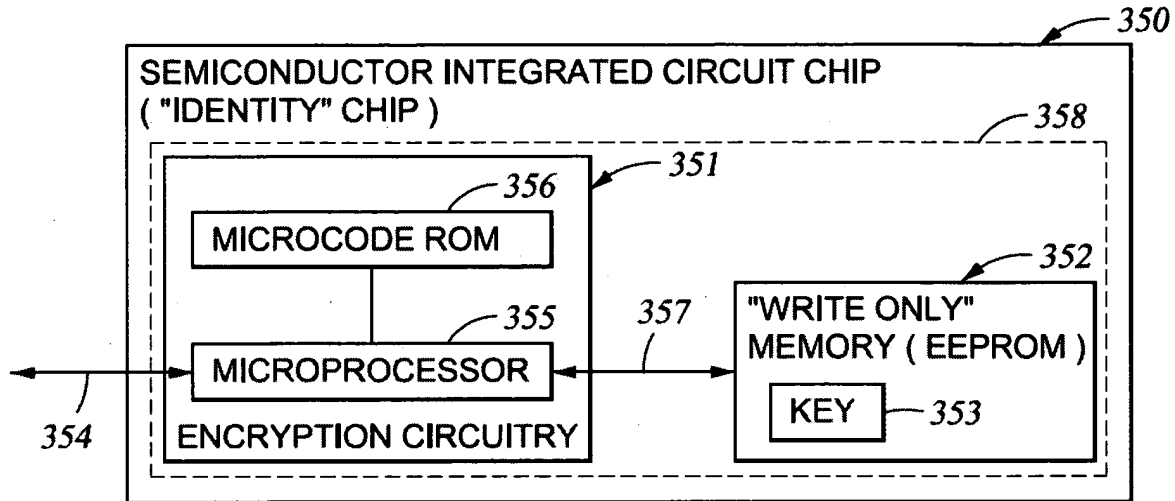
Claims 1 to 12 have been finally rejected, and are being appealed.

### **IV. STATUS OF AMENDMENTS**

No amendment was filed subsequent to final rejection.

### **V. SUMMARY OF CLAIMED SUBJECT MATTER**

The appellants' invention of claim 1 provides an electronic circuit chip (FIG. 31, item 350) including a memory (352) for storing information (353) defining an encryption procedure assigned to the electronic circuit chip; at least one input (354) to the electronic circuit chip for writing, to the memory, the information defining the encryption procedure assigned to the electronic circuit chip, and for receiving data to be encrypted by the encryption procedure assigned to the electronic circuit chip; encryption circuitry (351) for reading from the memory the information defining the encryption procedure assigned to the electronic circuit chip, and for



*Fig. 31*

encrypting the data from said at least one input to the electronic circuit chip according to the encryption procedure assigned to the electronic circuit chip, to produce encrypted data; and at least one output (354) from the electronic circuit chip for transmitting the encrypted data produced by the encryption circuitry. (Appellants' specification, page 3, line 17, to page 4, line 4.) The electronic circuit chip is constructed so that the information defining the encryption procedure assigned to the electronic circuit chip cannot be read from the memory from any output of the electronic circuit chip. (Appellants' specification, page 4, lines 4-6.) The electronic circuit chip is further constructed so that it is virtually impossible to recover the information in the memory by probing, inspection, or disassembly. (Appellants' specification, page 4, lines 6-8.) The electronic circuit chip includes a metal shielding layer (358) over the memory (352) so that the information stored in the memory cannot be read by visual inspection or probing. (Appellants' specification, page 4, lines 8-10.)

The appellants' invention of claim 7 provides an electronic circuit chip (FIG. 31, item 350) including a memory (352) for storing information; a microprocessor (355) coupled to the memory for reading information from the memory; at least one input (354) to the electronic circuit chip for receiving information to be written to the memory, and for receiving data to be processed by the microprocessor; and at least one output (354) from the electronic circuit chip for transmitting data processed by the microprocessor. (Appellants' specification, page 4, lines 11-16.) The electronic circuit chip is constructed so that information can be stored in the memory but not read from any output of the electronic circuit chip, and the microprocessor is programmable for encrypting data in accordance with an encryption procedure defined by information (353) that can be stored in the memory but not read from any output of the electronic circuit chip. (Appellants' specification, page 4, lines 16-20.) The electronic circuit chip is constructed so that it is virtually impossible to recover the information in the memory by probing, inspection, or disassembly. (Appellants' specification, page 4, lines 20-22.) The electronic circuit chip includes a metal shielding layer (358) over the memory so that the information stored in the memory cannot be read by visual inspection or probing. (Appellants' specification, page 4, line 22 to page 5, line 1.)

The appellants' invention of claim 12 includes the elements of claim 7, as summarized above, and in addition, the electronic circuit chip is a monolithic semiconductor integrated circuit chip. (Appellants' specification, page 77, lines 3-6.) The memory is an electrically erasable and programmable read-only memory (EEPROM 352) with a metal shielding layer (358) over the memory. (Appellants' specification, page 77, lines 6-10.) The metal shielding layer over the

memory is an upper layer of metal on the electronic circuit chip. (Appellants' specification, page 79, lines 7-11.) The microprocessor is programmed to read an encryption key (353) from the memory, and to compute the encrypted data using the encryption key. (Appellants' specification, page 79, lines 2-5.)

As described in the Appellants' specification, page 78 line 16 to page 79 line 11 (as amended):

FIG. 31 shows a preferred construction for the identity chip. The identity chip 350 includes encryption circuitry 351 and a "write-only" EEPROM memory 352 for storing at least one key 353. The key 353 can be written into the memory 352 from a data path 354 including external leads connected to the chip. The key 353 can be read from the memory 352 by the encryption circuitry, but the key cannot be read from the data path 354 or any other external leads connected to the chip. For example, the encryption circuitry 351 includes a microprocessor 355 and a microcode read-only memory (ROM) 356 storing microcode executed by the microprocessor. The microprocessor is programmed to recognize a command from the data path 354 for writing into the memory 352 a key from the bus 354. The microprocessor is also programmed to recognize a command from the data path 354 for receiving a number from the data path, reading the key 353 from the memory 352, encrypting the number with the key, and transmitting the encryption result onto the data path. The microprocessor, however, will not recognize any command for transmitting the key onto the data path 354 or any other leads of the chip. In this sense, the memory 352 is a "write-only" memory. Moreover, the EEPROM memory 352 and at least the internal data path 357 to the memory 352 are covered by an upper layer of metal 358 (shown in dashed lines in FIG. 31) on the chip 350 so that it is virtually impossible for the key to be recovered by probing, inspection, disassembly, or "reverse engineering" of the chip.

## **VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

1. Whether claims 1, 3-7, 9, and 12 are unpatentable under 35 U.S.C. 103(a) over Best (U.S. Patent 4,465,901) in view of Rigal (U.S. Patent 5,881,155).

2. Whether claims 2, 8, 10, and 11 are unpatentable under 35 U.S.C. 103(a) over Best (U.S. Patent 4,465,901) and Rigal (U.S. Patent 5,881,155) further in view of Little et al. (U.S. Patent 5,998,858).

## **VII. ARGUMENT**

The policy of the Patent and Trademark Office has been to follow in each and every case the standard of patentability enunciated by the Supreme Court in Graham v. John Deere Co., 148 U.S.P.Q. 459 (1966). M.P.E.P. § 2141. As stated by the Supreme Court:

Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined. Such secondary considerations as commercial success, long felt but unsolved needs, failure of others, etc., might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented. As indicia of obviousness or nonobviousness, these inquiries may have relevancy.

148 U.S.P.Q. at 467.

The problem that the inventor is trying to solve must be considered in determining whether or not the invention would have been obvious. The invention as a whole embraces the structure, properties and problems it solves. In re Wright, 848 F.2d 1216, 1219, 6 U.S.P.Q.2d 1959, 1961 (Fed. Cir. 1988).

**1. Claims 1, 3-7, 9, and 12 are patentable under 35 U.S.C. 103(a) over Best (U.S. Patent 4,465,901) in view of Rigal (U.S. Patent 5,881,155).**

**(a) Scope and Content of the Prior Art**

Best discloses a microprocessor for executing computer programs which are stored in cipher to prevent software piracy. Such a crypto-microprocessor deciphers the enciphered program piecemeal as it executes it, so that a large enciphered program can be securely executed without disclosing the deciphered program or associated data to persons who have access to the wiring of the computer in which the crypto-microprocessor is a component. Such a device may process valuable proprietary programs and data files which are distributed in cipher on videodiscs, semiconductor, or other media without risk of software piracy. Various methods of encryption may be used including methods which result in the cipher of a byte being a complicated function of the byte's address in memory. Each crypto-microprocessor chip may use a unique cipher key or tables for deciphering the program, so that a program that can be executed in one chip cannot be run in any other microprocessor. (Best, Abstract.) A typical crypto-microprocessor (CMP) is schematically shown as box 16 in FIG. 3. CMP 16 executes the enciphered program in memory 12 by addressing program portions via address bus 13, deciphering a program portion in deciphering circuit 43, and executing in processing circuit 3 the deciphered instructions obtained from circuit 4. The CMP may be constructed as an integrated circuit chip as shown in FIG. 15. (Best, Col. 4, lines 46-53). Deciphering circuit 4 is shown in greater detail in FIGS. 1, 8-13, 17, 21, and 23, and is comprised of various elements depending on the cipher method used. (Best, Col. 5, lines 11-14.) Deciphering in CMP 16 may be

controlled by a cipher key stored in a key register (register 5 in FIG. 4), or by one or more tables (boxes 32 in FIG. 11), or by one or more matrices (boxes 92 and 93 in FIG. 10) or by an arrangement of crossed wires (wires 34 in FIG. 11.) (Best, Col. 5, lines 17-21.) In the version shown in FIG. 1, deciphering of program bytes and enciphering/deciphering of data bytes is done by exclusive-ORing the byte to be enciphered or deciphered with a scrambling function of its bus 82 address. This exclusive-ORing is done by gates 28 for enciphering of output being written to memory 12, and by gates 29 by deciphering of input being read from memory. (Best, Col. 13, lines 14-21.)

Rigal discloses a security device for preventing access to confidential information stored in a semiconductor chip, referred to as the protected chip. The security device comprises a second semiconductor chip, referred to as the protective chip, with the two chips facing each other and being coupled to each other by communication terminals. The protected chip is coupled to external circuits via the protective chip, and the two semiconductor chips are separated by a semiconductor resin having a non-homogeneous electrical resistivity. The protective chip is provided with means for determining, at least from the measured resistances, an encryption key intended to be communicated to the protected chip to protect the confidential information. (Abstract.) The protected chip 10 may be a commonly available microcontroller (e.g., a microprocessor without internal memory, as made by Intel, Motorola, Texas Instruments, for example) provided with an electrically erasable memory (EEPROM or flash EPROM), a volatile memory (RAM) and encryption capabilities. (Rigal, Col. 4, lines 56-61.)



**(b) Differences between the Prior Art and the Claims at Issue**

Each of the independent claims 1 and 7 recite “a metal shielding layer over the memory so that the information stored in the memory cannot be read by visual inspection or probing.” The Final Official Action (mailed 12/23/2004) recognizes that Best “does not specifically mention a metal shielding layer over the memory.” The Final Official Action (page 3 and page 6) cites Rigal FIGS. 5 and 6 and col. 6, lines 30-37 for disclosing a guard ring 50. Rigal col. 6, lines 30-37 say:

In the second embodiment shown in FIGS. 5 and 6, a guard ring 50 is formed between chips 10 and 20 to surround and thereby protect the communication terminals 30. Guard ring 50 is a metallic layer used to electrically isolate the protected chip from external influences. Its specific dimensions are not of particular importance. For example, guard ring 50 can be formed at the periphery of the protected chip 10 and on a surface of the protective chip.

The Final Official Action suggests that the guard ring 50 of Rigal is a metal shielding layer over a memory. The appellants respectfully disagree. The guard ring is not shown or described as being over a memory. It is shown in Rigal FIGS. 5 and 6 and described as being a ring formed at the periphery of the protected chip 10 and on a surface of the protective chip 20. Presumably the memory containing the confidential information in Rigal would not be at the periphery of the protected chip 10, because the periphery of the protected chip would be a less secure location on the protected chip 10. Presumably the guard ring 50 is at the periphery of the protected chip 10 as shown in FIGS. 5 and 6 because electrical signals are conveyed between the

chips in the region surrounded by the guard ring. These electrical signals are conveyed through the regions 23 and 30 in FIG. 5, which are surrounded and not covered by the guard ring 50. As shown in the cross-section of FIG. 6, most of the guard ring 50 does not even overlap the protected chip 10. Moreover, the confidential information is said to be stored in the protected chip, and the protected chip and the protective chip are said to be separated by a semiconductor resin. (Abstract). In contrast, the appellants' claims call for the metal layer to be part of the chip, such as a layer on the chip, that contains the memory and the encryption circuitry such as the microprocessor.

**(c) The subject matter of the claims would not have been obvious in view of the differences.**

The subject matter of the appellants' claims would not have been obvious in view of the proposed combination of Rigal and Best, because neither Rigal nor Best discloses that a memory on an electronic circuit chip and containing information defining an encryption procedure assigned to an electronic circuit chip should be protected by a metal shielding layer over the memory so that the information stored in the memory cannot be read by visual inspection or probing. Where the prior art references fail to teach a claim limitation, there must be "concrete evidence" in the record to support an obviousness rejection. "Basic knowledge" or "common sense" is insufficient. *In re Zurko*, 258 F.3d 1379, 1385-86, 59 U.S.P.Q.2d 1693, 1697 (Fed. Cir. 2001).

Moreover, it is not seen where the cited art provides sufficient motivation for modifying a

proper combination of Best and Rigal to result in the appellants' invention of claims 1, 3-7, 9, or 12. Best is directed to a microprocessor for executing computer programs which are stored in cipher to prevent software piracy. This objective is different from the appellants' objective of providing a reasonably secure electronic circuit chip that can be given a unique identity by including in the electronic circuit chip a memory for storing information defining an encryption procedure assigned to the electronic circuit chip. Rigal is directed to a security device for preventing access to confidential information stored in a protected semiconductor chip. The security device comprises a second semiconductor chip with the two chips facing each other and being coupled to each other by communication terminals, and an encryption key encoded in a plurality of resistances in a semiconductor resin between the two semiconductor chips. It is not seen where Rigal would provide motivation to arrive at the appellants' claimed invention by discarding the second semiconductor chip and semiconductor resin and instead using a metal layer over the EEPROM on the protected chip to protect the confidential information in the EEPROM. Rigal appears entirely satisfactory for its intended purpose, and the proposed modification is in the opposite direction from Rigal's objective and inconsistent with Rigal's disclosure as a whole.

It is improper to attempt to establish obviousness by using the appellants' specification as a guide to combining different prior art references to achieve the results of the claimed invention. *Orthopedic Equipment Co., Inc. v. United States*, 702 F.2d 1005, 1012, 217 U.S.P.Q. 193, 199 (Fed. Cir. 1983). Hindsight reconstruction, using the appellants' specification itself as a guide, is improper because it fails to consider the subject matter of the invention "as a whole"

and fails to consider the invention as of the date at which the invention was made. The critical inquiry is whether there is something in the prior art as a whole to suggest the desirability, and thus the obviousness, of making the combination. *In re Dembiczak*, 175 F.3d 994, 999-1000, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999)(actual evidence and particular findings need to support the PTO's obviousness conclusion); *Interconnect Planning Corp. v. Feil*, 774 F.2d 1132, 1138, 227 U.S.P.Q. 543, 547 (Fed. Cir. 1985) ("The invention must be viewed not with the blueprint drawn by the inventor, but in the state of the art that existed at the time."); *In re Fritch*, 972 F.2d 1260, 1266, 23 U.S.P.Q.2d 1780, 1784 (Fed. Cir. 1992)("It is impermissible to use the claimed invention as an instruction manual or 'template' to piece together the teachings of the prior art so that the claimed invention is rendered obvious."); *Fromson v. Advance Offset Plate, Inc.*, 755 F.2d 1549, 1556, 225 U.S.P.Q. 26, 31 (Fed. Cir. 1985) (nothing of record plainly indicated that it would have been obvious to combine previously separate lithography steps into one process). See, for example, *In re Gordon et al.*, 733 F.2d 900, 902, 221 U.S.P.Q. 1125, 1127 (Fed. Cir. 1984) (mere fact that prior art could be modified by turning apparatus upside down does not make modification obvious unless prior art suggests desirability of modification); *Ex Parte Kaiser*, 194 U.S.P.Q. 47, 48 (PTO Bd. of Appeals 1975) (Examiner's failure to indicate anywhere in the record his reason for finding alteration of reference to be obvious militates against rejection).

### **Claims 1 and 3-6**

Claim 1 defines at least one input to the electronic circuit chip for receiving data to be

encrypted by the encryption procedure assigned to the electronic circuit chip; encryption circuitry for reading from the memory the information defining the encryption procedure assigned to the electronic circuit chip, and for encrypting the data from said at least one input to the electronic circuit chip according to the encryption procedure assigned to the electronic circuit chip, to produce encrypted data; and at least one output from the electronic circuit chip for transmitting the encrypted data produced by the encryption circuitry. Dependent claims 3-6 include these limitations by reference to their base claim 1. It is not seen where Best or Rigal disclose these limitations.

Page 2 of the Final Official Action says that Best discloses one input (see Best col. 6, lines 48-53), one output (see Best col. 7, lines 45-47), an encryption program for encryption/decryption procedures (see Best col. 4, lines 41-43; col. 7, lines 49-53), and the capability to both encrypt and decrypt data (see Best col. 7, lines 49-53.) However, it is not seen where data from an input of the chip is encrypted and put on an output of the chip. For example, data encryption in Best is said to be for “temporary external storage of portions of partially processed data without compromising its contents.” (Best, col. 7, lines 48-49.) In contrast, the data encryption in the appellants’ electronic circuit chip is for giving the electronic circuit chip a unique identity.

### **Claim 12**

Independent claim 12 further defines “wherein the electronic circuit chip is a monolithic semiconductor integrated circuit chip, the memory is an electrically erasable and programmable

read-only memory, and the metal shielding layer over the memory is an upper layer of metal on the electronic circuit chip; ....” It is not seen where this is disclosed in Best or in Rigal. In Rigal FIG. 6, the guard ring 50 is a layer of metal on the protective chip 20, not the protected chip 10 which may include a memory.

Claim 12 defines a re-programmable tamper-resistant circuit chip that does not require any special encapsulation of the chip in order to make it tamper resistant. The complexity of the cited references themselves evidence a long felt but unsolved need to provide such an identity chip that does not require any special encapsulation of the chip in order to make it tamper resistant.

**2. Claims 2, 8, 10, and 11 are patentable under 35 U.S.C. 103(a) over Best (U.S. Patent 4,465,901) and Rigal (U.S. Patent 5,881,155) further in view of Little et al. (U.S. Patent 5,998,858).**

Claims 2, 8, 10, and 11 are dependent claims. Each of these claims further includes a limitation that the electronic circuit chip is a monolithic semiconductor integrated circuit chip. Page 9 of the Final Official Action says: “Best’s chip is not monolithic semiconductor integrated circuit chip.” The Final Official Action cites Little for disclosing “a monolithic semiconductor chip 135 that may comprise a host of circuit elements such as memory, microprocessors, multiplexing circuitry and electrostatic discharge protection circuitry.” (Little, col. 5, lines 2-5.)

Although monolithic semiconductor integrated circuit chips of various kinds are well known, the pertinent issue is what circuits and functions are integrated on a single chip. The appellants have taught that by including particular circuits and functions on a single chip, there is

provided a reasonably secure identity chip. This reasonably secure identity chip can be manufactured using standard integrated circuit processing techniques, without the expense of the complexity disclosed in Best, Rigal and Little. Such a reasonably secure identity chip would not have been obvious from Best, Rigal and Little.

### **Claims 10 and 11**

Claims 10 and 11 further define that the memory is an electrically erasable and programmable read-only memory, and the metal shielding layer over the memory is an upper layer of metal on the electronic circuit chip. The memory in Little is a static random access memory (SRAM), and not an electrically erasable and programmable read-only memory (EEPROM). In Rigal FIG. 6, the guard ring 50 is a layer of metal on the protective chip 20, not the protected chip 10 which may include a memory.

Claims 10 and 11 define a re-programmable tamper-resistant circuit chip that does not require any special encapsulation of the chip in order to make it tamper resistant. The complexity of the cited references themselves evidence a long felt but unsolved need to provide such an identity chip that does not require any special encapsulation of the chip in order to make it tamper resistant.

Serial No.: 10/058,651  
Appeal Brief

In view of the above, the rejection of claims 1 to 12 should be reversed.

Respectfully submitted,

*23 March 2005*



Richard C. Auchterlonie  
Reg. No. 30,607

NOVAK DRUCE & QUIGG, LLP  
1000 Louisiana, Suite 5320  
Houston, TX 77002  
713-751-0655



## **VIII. CLAIMS APPENDIX**

The claims involved in this appeal are as follows:

1. An electronic circuit chip comprising:

a memory for storing information defining an encryption procedure assigned to the electronic circuit chip;

at least one input to the electronic circuit chip for writing, to the memory, the information defining the encryption procedure assigned to the electronic circuit chip, and for receiving data to be encrypted by the encryption procedure assigned to the electronic circuit chip;

encryption circuitry for reading from the memory the information defining the encryption procedure assigned to the electronic circuit chip, and for encrypting the data from said at least one input to the electronic circuit chip according to the encryption procedure assigned to the electronic circuit chip, to produce encrypted data; and

at least one output from the electronic circuit chip for transmitting the encrypted data produced by the encryption circuitry;

wherein the electronic circuit chip is constructed so that the information defining the encryption procedure assigned to the electronic circuit chip cannot be read from the memory from any output of the electronic circuit chip; and

wherein the electronic circuit chip is constructed so that it is virtually impossible to recover the information in the memory by probing, inspection, or disassembly; and

which includes a metal shielding layer over the memory so that the information stored in the memory cannot be read by visual inspection or probing.

2. The electronic circuit chip as claimed in claim 1, wherein the electronic circuit chip is a monolithic semiconductor integrated circuit chip.

3. The electronic circuit chip as claimed in claim 1, wherein the memory is an electrically erasable and programmable read-only memory.

4. The electronic circuit chip as claimed in claim 1, wherein said encryption circuitry includes a microprocessor for computing the encrypted data.

5. The electronic circuit chip as claimed in claim 4, wherein the microprocessor is constructed to execute an encryption program stored in the memory, and the encryption program defines the encryption procedure assigned to the electronic circuit chip.

6. The electronic circuit chip as claimed in claim 4, wherein said microprocessor is programmed to read an encryption key from the memory, and to compute the encrypted data using the encryption key, and the encryption key defines the encryption procedure assigned to the electronic circuit chip.

7. An electronic circuit chip comprising:

- a memory for storing information;
- a microprocessor coupled to the memory for reading information from the memory;
- at least one input to the electronic circuit chip for receiving information to be written to the memory, and for receiving data to be processed by the microprocessor; and
- at least one output from the electronic circuit chip for transmitting data processed by the microprocessor;

wherein the electronic circuit chip is constructed so that information can be stored in the memory but not read from any output of the electronic circuit chip, and the microprocessor is programmable for encrypting data in accordance with an encryption procedure defined by information that can be stored in the memory but not read from any output of the electronic circuit chip;

wherein the electronic circuit chip is constructed so that it is virtually impossible to recover the information in the memory by probing, inspection, or disassembly; and

which includes a metal shielding layer over the memory so that the information stored in the memory cannot be read by visual inspection or probing.

8. The electronic circuit chip as claimed in claim 7, wherein the electronic circuit chip is a monolithic semiconductor integrated circuit chip.

9. The electronic circuit chip as claimed in claim 7, wherein the memory is an

electrically erasable and programmable read-only memory.

10. The electronic circuit chip as claimed in claim 1, wherein the electronic circuit chip is a monolithic semiconductor integrated circuit chip, the memory is an electrically erasable and programmable read-only memory, and the metal shielding layer over the memory is an upper layer of metal on the electronic circuit chip.

11. The electronic circuit chip as claimed in claim 7, wherein the electronic circuit chip is a monolithic semiconductor integrated circuit chip, the memory is an electrically erasable and programmable read-only memory, and the metal shielding layer over the memory is an upper layer of metal on the electronic circuit chip.

12. An electronic circuit chip comprising:  
a memory for storing information;  
a microprocessor coupled to the memory for reading information from the memory;  
at least one input to the electronic circuit chip for receiving information to be written to the memory, and for receiving data to be processed by the microprocessor; and  
at least one output from the electronic circuit chip for transmitting data processed by the microprocessor;  
wherein the electronic circuit chip is constructed so that information can be stored in the memory but not read from any output of the electronic circuit chip, and the microprocessor is

programmable for encrypting data in accordance with an encryption procedure defined by information that can be stored in the memory but not read from any output of the electronic circuit chip;

wherein the electronic circuit chip is constructed so that it is virtually impossible to recover the information in the memory by probing, inspection, or disassembly; and

which includes a metal shielding layer over the memory so that the information stored in the memory cannot be read by visual inspection or probing;

wherein the electronic circuit chip is a monolithic semiconductor integrated circuit chip, the memory is an electrically erasable and programmable read-only memory, and the metal shielding layer over the memory is an upper layer of metal on the electronic circuit chip; and

wherein the microprocessor is programmed to read an encryption key from the memory, and to compute the encrypted data using the encryption key, and the encryption key defines the encryption procedure assigned to the electronic circuit chip.